



Minister van Justitie en Veiligheid

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl

Datum
23 mei 2024

Ons kenmerk
5443858

nota

Toekomstvisie Cyberweerbaarheidsnetwerk

1. Aanleiding

In 2017 adviseerde de Cyber Security Raad (CSR) om het Landelijk Dekkend Stelsel (LDS) in te richten. Een stelsel dat als doelstelling heeft om organisaties in staat te stellen slagkracht te verhogen door cybersecurityinformatie breed, efficiënt en effectief met elkaar te delen. In 2018 ging samenwerking binnen dit stelsel van start.

In de Nederlandse Cybersecuritystrategie 2022-2028 (NLCS) zijn de ambities en acties voor een digitaal veilige samenleving opgenomen.¹ Het kabinet beschrijft in een van de acties dat in samenwerking met private partners een bouwplan wordt opgesteld dat het kabinet in staat stelt om samen met het bedrijfsleven de digitale weerbaarheid te verhogen. Hiermee wil het kabinet ook een grote behoefte van de private partners in. Onderdeel van dit bouwplan is een overzicht van de huidige staat van het LDS om inzicht te creëren in de initiatieven die reeds zijn ontwikkeld en de huidige leemtes in het LDS.

2. Geadviseerd besluit

Aan de minister wordt gevraagd:

- Kennis te nemen van en in te stemmen met de Kamerbrief Toekomstvisie Cyberweerbaarheidsnetwerk;
- kennis te nemen van en in te stemmen met de Rapportage Toekomstvisie Cyberweerbaarheidsnetwerk;
- in te stemmen met verzending van de Kamerbrief en de Rapportage Cyberweerbaarheidsnetwerk aan de Tweede Kamer.

3. Kernpunten

De Kamerbrief en Rapportage geven inzicht in de tot stand gekomen toekomstvisie voor het Landelijk Dekkend Stelsel. De naam van het Landelijk Dekkend Stelsel zal veranderd worden naar 'Cyberweerbaarheidsnetwerk'. Deze naamwijziging is een resultaat van overleg tussen de publiek-private partners binnen het stelsel.

De kernfunctie van het huidige Landelijk Dekkend Stelsel is het delen van dreigingsinformatie. Om de cyberweerbaarheid van organisaties in Nederland

¹ Kamerstukken II, 2022-23, 26643, nr. 925

te verhogen is meer nodig dan slechts het delen van informatie. Onder meer de functies van kennisuitwisseling en het opleiden, trainen en oefenen van reageren op cyberincidenten worden toegevoegd aan de functies van het Cyberweerbaarheidsnetwerk. Er worden samenwerkingsafspraken tussen de publiek-private partners gemaakt, waarbij de regie over het netwerk bij de NCTV blijft liggen.

Datum

23 mei 2024

Ons kenmerk

5443858

Een zevental beleidskeuzes is gemaakt. Dit zijn de volgende punten: (1) De naam het stelsel wordt aangepast naar Cyberweerbaarheidsnetwerk; (2) Het aantal schakelorganisaties dient te worden uitgebreid om het bereik van het netwerk te vergroten; (3) De functie van informatiedeling wordt uitgebreid, waardoor de focus niet alleen op informatie ten tijde van een incident plaatsvindt, maar ook informatiedeling plaatsvindt vóór en na dat incidenten plaatsvinden; (4) Er worden functies aan het netwerk toegevoegd zoals als kennisuitwisseling en het opleiden, trainen en oefenen van reageren op cyberincidenten; (5) Samenwerkingsafspraken dienen gemaakt te worden om het vertrouwen en het wederkerig profijt van samenwerking door publieke en private partners te waarborgen; (6) De NCTV zal binnen het netwerk gaan optreden als centrale regiehouder; (7) Waar mogelijk worden initiatieven die raakvlak hebben met publiek-private samenwerking binnen het netwerk samengevoegd. Zo worden initiatieven geconsolideerd en kan ervoor gezorgd worden dat verschillende initiatieven goed op elkaar aan blijven sluiten. Hierbij wordt waar mogelijk de scope verbreed naar het Koninkrijk der Nederlanden.

4. Toelichting.

4.1 Politieke context

In de Voortgangsrapportage van de NLCS van 2023 is toegezegd dat het toekomstbeeld voor het Landelijk Dekkend Stelsel in het eerste kwartaal van 2024 wordt verstuurd aan de Tweede Kamer.² De Kamerbrief en de Rapportage voorzien hierin.

4.2 Krachtenveld en stakeholders

De Kamerbrief en Rapportage over de toekomstvisie zijn en worden in nauwe afstemming en samenwerking met de beleidsdepartementen, het NCSC (gezamenlijk met het DTC) als uitvoeringscoördinator én de netwerkpartners opgesteld en onderhouden. De werking van het netwerk wordt regelmatig geëvalueerd, zowel voor wat betreft resultaten, als wat betreft de wijze van uitvoering.

5. Informatie die niet openbaar gemaakt kan worden

5.1 Toelichting

De persoonsgegevens van de ambtenaren zijn niet openbaar ter bescherming van de persoonlijke levenssfeer.

² Voortgangsrapportage Nederlandse Cybersecuritystrategie, Oktober 2023